

**U.S. General Services Administration (GSA)**

**PRESIDENTIAL TRANSITION “HOT ISSUES” INFORMATION PAPER**

---

**SUBJECT:** *Login.gov*

**1. BACKGROUND:**

[Login.gov](#) is a collaboration between TTS and FAS Office of Integrated Technology Service (ITS) to operationalize a digital Consumer Identity Service to enable all government agencies to provide online services to consumers using digital consumer identities. This will create a consistent user experience across services with greater security, usability, privacy, and efficiency.

One common complaint is the inconsistent, difficult experience that the public has logging in and proving their identity when interacting with the government online. TTS's Office of 18F and a team of technologists from across the government are building an authentication tool for users who need to log in to government services. The project is undertaken with cooperation with the Office of Management and Budget and the National Institute of Standards and Technology. The project builds off the priorities in the Cybersecurity National Action Plan as well as the Cyber Information Security Act.

a. Issues:

- Timelines established are ambitious and require prompt coordination from many partners of GSA including FAS (Commissioner, Integrated Technology Service, and NCR Assisted Acquisition Service), the Office of Governmentwide Policy's Senior Procurement Executive, GSA IT, and the Office of General Counsel.
- Multi-agency cooperation is needed for the platform to be a success and achieve economies of scale.
- Procurement is very slow and not agile, causing delays to program. 5-6 more procurements will be required and more agility will be necessary to deliver successfully.
- Authority To Operate (ATO) process is also very slow and does not yield the benefits based on the level of effort.

**2. SCOPE AND EFFECT:**

a. Impact on GSA's Customers (Federal Agencies, State and Local Governments):

- A common platform makes it easier to leverage technology investments across the federal government.
- Agencies will be able to save their existing cost of developing and procuring identity services and managing user identities.
- Agencies can leverage and meet the guidelines for shared services as per EO 13681 Implementation Plan Draft.
- Agencies can avoid costs due to the rising complexity of building and operating software, the difficulty of running fraud detection models which protect the

public's data, and the extremely high cost of mitigation should a data breach occur.

- The Federal government can maintain a common user experience both in platform and support.
- Reduce the risk of vendor lock-in and increase the flexibility to replace vendors and upgrade identity services as technologies improve and security needs evolve.
- Federal Chief Information Security Officers can concentrate on agency-specific threats and vulnerabilities instead of on basic authentication.

b. Impact on the Private Sector Partners:

- Opportunity for the Login.gov team to partner with industry for expertise and innovation for identity services and authentication.

**3. ACTION(S) PLANNED OR REQUIRED:**

- Login.gov is building on lessons from pilot programs implemented in the United States, as well as successful efforts by other countries:
  1. Connect.gov
  2. MyUSA.gov
  3. GovUK Verify
- Login.gov is following current best practices --- and helping shape their future:
  1. Implementing National Strategy for Trusted Identities in Cyberspace (NSTIC) principles, which are the north star for identity policy since 2003.
  2. Working to ensure that we build and maintain a secure and resilient platform that is also interoperable, cost-effective and easy to use.
- Login.gov's strategic growth plan sets a goal to have multiple agencies integrated by FY18. The presidential transition will require multiple levels of leadership in GSA to work with the new political appointees in other agencies to drive integration of login.gov.

**4. KEY STAKEHOLDER INTEREST:**

**Congressional Interest:** There have been multiple efforts in the past few years to strengthen cybersecurity across the federal government. Congress passed the Cybersecurity Act (CISA) in October 2015 to strengthen the nation's cybersecurity, followed by OMB's Cybersecurity National Action Plan (CNAP) in February 2016 to identify short-term and long-term actions to empower "Americans to secure their online accounts by using additional security tools - like multi-factor authentication and other identity processing steps."

**5. FISCAL YEAR 2017/2018 BUDGET IMPACT:**

Login.gov has received an approved executive business case and associated five year funding from the GSA Investment Review Board. The Federal Citizen Services Fund is paying the cost of the pilot for the participating agencies. The Acquisition Services Fund is also investing in the development of the platform and those costs will be recovered in fees charged to user agencies at the conclusion of the pilot program. As the adoption of the program grows over the 5 year period, the overall cost savings for government will be substantial, allowing agencies to realize

higher performance at a lower cost. It is expected that the price will decline based on the agency adoption models that have been built.